UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,311	06/28/2004	David Arditti Modiano	T2151-9156US01	9860

181 7590 06/04/2007

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
06/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/500,311	ARDITTI MODIANO ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 June 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *19-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *19-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06/28/2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 19-38 have been examined.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claim 19 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

4. Claim 19 is directed to a group signature system enabling a group to produce a message accompanied by a signature. The examiner respectfully asserts that the claimed subject matter does not fall within the statutory classes listed in 35 USC 101. The claimed steps do not result in a tangible result. Claims 19 are rejected as being directed to an abstract idea. (i.e., producing non tangible result).[tangible requirement does require that the claim must recite more than a 101 judicial exception, in that the process claim must set forth a practical application of that 101 judicial exception to produce a real-world result, Benson, 409 U.S at 71-72, 175 USPQ at 676-77].Claims 20-31 are depend on claim 19 therefore they are rejected on the same reason.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

6. Claims 19-38 rejected under 35 U.S.C. 102(b) as being anticipated by Saito et al(hereinafter referred as Saito)US Patent No 6,161,183.

7. As per claim 19: Saito disclose a group signature system enabling a member (M) of a group (G) to produce a message (m) accompanied by a signature (S) for proving to a checker (2, 4) that the said message (m) originates from a member (M) of said group (G), using personalized data (z; Kz)(See col 5 lines 15-28 and Fig 1 step 11(i.e., user information)), characterized in that said system is electronic and includes an electronic hardware support (26)(See Fig 1 step 12(i.e., token)) and in that the said personalized data is integrated into said electronic hardware support (26)(See Fig 3 step 12 and col 9 line 62 through col 10 line 8).

8. As per claim 20: Saito disclose a group signature system characterized in that said hardware support includes encryption means (B3) for personalizing encrypted text (C) using the said personalized data (z; Kz) before the signature (S) of the message (m)(See Fig 6 step a and col 13 lines 27-38).

9. As per claim 21: Saito discloses a group signature system characterized in that said hardware support further includes means (B5) for combining the message (m) to be signed and the encrypted text (C) associated with said message (m) in the form of a concatenation of the message (m) with the encrypted text (C)(See Fig 13 steps 23-24 and col 5 lines 15-29).

10. As per claim 22: Saito disclose a group signature system wherein the hardware support further includes signature means (Sig-B6) for producing a signature of the message (m) with the personalized data (z; Kz) in any encrypted form (C) associated with said message (col 9 line 61 through col 10 line 8).

11. As per claim 23: Saito discloses a group signature system characterized in the said personalized data is an identifier (z) personal to the member (M), and in that the said electronic hardware support (26) includes an encryption key (K) common to all members of the group (G), and encryption means (B3) for encrypting (C) the identifier (z) with the said encryption key (See col 7 lines 1-12).

12. As per claim 24: Saito discloses a group signature system characterized in that encryption means (B3) encrypts the text (C) with the identifier (z) and a random number (r)(col 3 lines 47-58).

13. As per claim 25: Saito A group signature system characterized in that the said personalized data is a diversified encryption key (Kz) specific to each member (M) of the group (G), and in that encryption means (B3) encrypts the text (C) using at least one data (r) with the said encryption key (Kz)(See col 7 lines 1-12).

14. As per claim 26: Saito discloses a group signature system according to claim 26, characterized in that the said data (r) includes a random number (col 3 lines 47-58).

15. As per claim 27: Saito discloses a group signature system characterized in that the encryption means (B3) uses a secret key encryption algorithm (K)(col 3 lines 47-58).

16. As per claim 28: Saito discloses a group signature system hardware support wherein the encryption means (B3) use either a public key encryption algorithm RSA (Rivest, Shamir, Adleman) or an AES (Advanced Encryption Standard) public encryption algorithm (col 5 lines 2-6).

17. As per claim 29: Saito discloses a group signature system characterized in that the signature means (B6) uses a private key signature algorithm (SK)(See Fig 3 step 23).

18. As per claim 30: Saito discloses a group signature system characterized in that the private key signature algorithm is of the RSA type (Rivest, Shamir, Adleman)(col 5 lines 2-6).

19. As per claim 31: Saito discloses a group signature system characterized in that said hardware support comprises a portable communicating device (26)(See Fig step 12).

20. As per claim 32: Saito discloses a group signature system characterized in that said portable communicating device is a smart card (26)(See Fig 1 step 12).

21. As per claim 33: Saito discloses a method for checking a message (m) sent by a member (M) of a group (G) accompanied by a signature (S) wherein the message (m) authentication the signature to indicated that the message originates from a member of the group, comprises producing the signature (S) of the message (m) with a private key (SK) common to members (M) of the group (G) and integrating personalized data (z; KZ) electronic hardware support (26) into the message (See col 7 lines 1-12,col 5 lines 15-28 and Fig 1 steps 11,12), transmitting the message with the authenticated signature

to a user of the system (2,6) without needing to supply proof to the user that the member (M) belongs to the said group (G)(See col 9 lines 62-67 and col 11 lines 21-37).

22. As per claim 34: Saito discloses a method for checking a message (m)characterized in that the message is checked using a public key corresponding to the said private key (SK)(See col 11 lines 21-55).

23. As per claim 35: Saito discloses a method for opening a signature (S) produced by a group signature system which enables a member (M) of a group (G) to produce a message (m) accompanied by the signature (S) so as to authenticate the signature (S) for a user of the system comprising the steps of: making correspondence data between the identities of members (M) of the group (G) and their personalized data available, before the signature (See col 7 lines 1-7,col 13 lines 56-64); decrypting the personalized data received from an electronic hardware support (26) for which the signature is to be opened(See col 9 line 62 through col 10 line 8); and opening the signature when the decrypted personalized data corresponds to the identity of the member (M) of the group (G)(See co 7 lines 1-7, col 13 lines 27-38).

24. As per claim 36: Saito discloses a method for adapting an electronic hardware support (26) for a group signature system which enables a member (M) of a group (G) to produce a message (m) accompanied by a signature (S) to authenticate the signature (S) for a user of the system wherein the hardware support is personalized to a member (M) of the group, characterized in that it comprises steps consisting of: producing personalized data (z; Kz) to be used for the said electronic hardware support (26) to be

personalized(See Fig 1 step 11(i.e., user information)); and registering this personalized data with a private signature key (SK) in the said hardware support(See Fig 3 step 23(i.e., token private key)).

25. As per claim 37: Saito discloses a group signature system, comprising a terminal (10), said terminal including means for reading a portable communicating device issued to a member (M) of a group by a trusted authority, said device being personalized to the member (M) with personalized data integrated into the device in the form of an identifier (z, Kz) so as to be capable of producing a message and signature associated with the group (See col 7 lines 1-7,col 13 lines 56-64); said device including encryption means for making a personalized encrypted text using the personalized data before the signature of the message and means for making a combination of the message to be signed and the encrypted text associated with the message in the form of a concatenation of the message and the encrypted text(See col 9 through col 10 line 8).

26. As per claim 38: Saito discloses a group signature system wherein said device further includes means for producing the signature associated with the message in encrypted form using the personalized data and wherein users within the system include commercial entities which require a signature to be authenticated (See col 6 lines 57-67).

Conclusion

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser,can be reached on 5712738300. The fax phone number for the organization where this application or proceeding is assigned is 571-272-4195.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew
05/24/07

Art Unit 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

5/26/07